CRIMES CIBERNÉTICOS

Jéssica de Jesus Almeida [1]
Allana Barbosa Mendonça [2]
Gilmar Passos do Carmo [3]
Kendisson Souza Santos [4]
Luana Munique Meneses Silva [5]
Roberta Rayanne Dória de Azevedo [6]

Direito

cadernos de graduação
ciências humanas e sociais

ISSN IMPRESSO 1980-1785
ISSN ELETRÔNICO 2316-3143

RESUMO

O presente trabalho objetiva realizar uma breve análise didática a respeito dos chamados "crimes cibernéticos". Para tanto, se faz necessário entender o âmbito em que se insere essa nova modalidade de prática delitiva, ou seja, o ambiente virtual. Importante destacar, ainda, que a fim de combater a criminalidade e a impunidade dos delitos praticados no ambiente virtual, surgiu a Lei dos Crimes Cibernéticos, nacionalmente conhecida por "Lei Carolina Dieckmann", de número 12735, de 3 de dezembro de 2012. Essa legislação elencou as condutas consideradas penalmente típicas, não reconhecendo, contudo, a existência de diversas condutas delitivas praticadas no mundo virtual. Destarte, o legislador ao não considerar dadas condutas como sendo, propriamente, crimes cibernéticos, estas passaram, todavia, a serem conhecidas doutrinariamente como "crimes virtuais impróprios". Ademais, o presente estudo busca, precipuamente, analisar o conteúdo da referida Lei e de todas as alterações trazidas por ela ao ordenamento pátrio brasileiro, amealhando-se, ainda, julgados recentes, com o fito de conhecer o entendimento dos Tribunais Superiores pátrios acerca dessa temática.

Palavras-chave

Crimes Cibernéticos. Lei "Carolina Dieckmann". Crimes Virtuais.

ABSTRACT

This paper aims to conduct a brief training analysis about the so-called "cyber crime". Therefore, it is necessary to understand the context in which it appears this new type of unlawful activities, ie the virtual environment. Importantly, though, that in order to combat crime and impunity for crimes committed in the virtual environment, the Law on Cybercrime, nationally known as "Carolina Dieckmann Law" emerged, number 12735, of December 3, 2012. This legislation listed the criminal behavior considered typical, not recognizing, however, the existence of several criminal acts committed in the virtual world. Thus the legislature to conduct not considered as given, properly, cyber crime, these have, however, to be known as doctrinally "unfit cyber crimes." In addition, this study aims, primarily, that analyze the content of the Law and all the changes introduced by it to the Brazilian paternal order, if garnering-also judged recent, with the aim of knowing the understanding of the Superior Courts patriotic about this theme.

KEYWORDS

Cyber Crime. "Carolina Dieckmann Law".

1 INTRODUÇÃO

Segundo Chaves (apud SILVA, 2003, p.19), Cibernética é a "ciência geral dos sistemas informantes e, em particular, dos sistemas de informação". Assim, por meio do conceito analítico de crime, pode-se chegar à conclusão de que "crimes cibernéticos" são todas as condutas "típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática" (SCHMIDT, 2014, [n.p.]).

Outrossim, valiosas são as lições de Fabrício Rosa (2002 apud SCHMIDT, 2014, [n.p.]), acerca da conceituação do crime de informática. Vejamos:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe does elementos indissolúveis:

> contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, [entre outros].

Partindo de uma perspectiva baseada na "Convenção sobre o *Cibercrime* de Budapeste", realizada no ano de 2001, pode-se aduzir que os crimes de informática são aqueles perpetrados por meio dos computadores, contra eles ou através deles, de modo que a maioria dos crimes é praticada por meio do sistema de internet (SCHMIDT, 2014 apud CASTRO, 2003).

Ademais, tratando-se de antecedentes históricos, podemos dizer que os aparecimentos dos primeiros casos de crimes informáticos ocorreram na década de 1960, os quais, nada mais eram, do que delitos em que o infrator manipulava, sabotava, espionava ou exercia abuso abusivo de computadores e sistemas.

E então, foi apenas a partir do ano de 1980, que houve um aumento das ações criminosas, que passaram a refletir em, por exemplo, manipulações de caixas bancários, abusos de telecomunicação, pirataria de programa e pornografia infantil, sendo que o último fato vem preocupando consideravelmente os cidadãos (OLIVEIRA JÚNIOR, 2013).

Um assunto relativamente novo dentro do âmbito de Lei, digo ainda, dentre os rols de condutas criminosas, e de todos conjuntamente, é a criminalidade cibernética.

Ressalte-se que no ano de 2012 fora sancionada uma Lei que trata do caso em tela, a chamada "Lei Carolina Dieckmann" como ficou conhecida a Lei Brasileira nº 12.737/2012. Este dispositivo legal fora sancionada em 3 de dezembro de 2012, pela então Presidenta Dilma Rousseff, a qual promoveu, entretanto, algumas alterações no Código Penal Brasileiro, tipificando os chamados "delitos ou crimes informáticos". A lei acresceu os artigos 154-A e 154-B e alterou os artigos 266 e 298 do Código Penal brasileiro (FRANCESCO, 2014).

A referida legislação é oriunda do Projeto de Lei nº 2793/2011, apresentado em 29 de novembro de 2011, pelo Deputado Paulo Teixeira (PT-SP), que tramitou em regime de urgência e em tempo *record* no Congresso Nacional, em comparação com outros projetos sobre delitos informáticos que as casas de leis apreciavam (como, por exemplo, o PL 84/1999, a "Lei Azeredo", também transformado em lei ordinária 12.735/2012 em 3 de dezembro de 2012) (VIEIRA; ALVES, 2013).

A nova lei ganhou notoriedade, porque antes mesmo de publicada e sancionada, já havia recebido o nome de "Lei Carolina Dieckmann". Tal apelido se deu em razão da repercussão do caso no qual a atriz teve seu computador invadido e seus arquivos pessoais subtraídos, inclusive com a publicação de fotos íntimas que rapidamente se espalharam pela internet por meio das redes sociais (OLIVEIRA JÚNIOR, 2013).

Uma análise, mesmo que superficial, do atual panorama sociológico global, demonstra a grande mudança de paradigmas sociais, e dessa maneira induz a conclusão de uma necessidade de se aprimorar a legislação penal informática, a fim de se evitar à impunidade dos chamados delitos informáticos próprios, ou seja, aqueles que só podem ser praticados por meio da internet.

É de se notar, também, a importância que os sistemas informáticos possuem no atual momento social, ressaltando que a maioria das pessoas, físicas ou jurídicas, depende do seu dispositivo informatizado, que variam de um simples pendrive ou celular, até um computador com banco de dados sigilosos de uma empresa (BRITO, 2013).

No tocante à segurança informática, portanto, entendida como a disponibilidade, confidencialidade e integridade das informações dos usuários, há tempo já clamava por proteção jurídico-penal, já que a "violência" nesse meio vem evoluindo a longos passos.

Assim, com o advento dos mencionados dispositivos legais, os usuários das novas tecnologias da informação passaram a ficar amparados pela Lei, caso venham a sofrer ataques semelhantes ao que sofreu a atriz Carolina Dieckmann.

Diga-se, então, que a Lei vem sofrendo críticas de juristas, peritos, especialistas e profissionais de segurança da informação, pois seus dispositivos são amplos, confusos e podem gerar dupla interpretação, ou mesmo interpretação subjetiva, o que pode ser utilizado para enquadramento criminal de condutas triviais ou mesmo para a defesa e respaldo de infratores cibernéticos, o que tornaria a lei injusta e ineficaz.

A corrente oposicionista defende, ainda, que as penas são pouco inibidoras, sendo muitas situações enquadráveis nos procedimentos dos Juizados Especiais, o que poderia contribuir para a não eficiência no combate ao crime cibernético no Brasil.

No tocante a atuação da polícia em crimes de computação, crimes dessa natureza requer investigação especializada e ação efetiva. Infeizmente, não existem no Brasil policiais preparados para combater esse tipo de crime, faltando, pois, visão, planejamento, preparo e treinamento (MIRANDA, 2013).

Em contrapartida, o nível de *hackeres* no Brasil vem crescendo a largos passos e consequentemente trazendo prejuizo para as empresas e para os cidadãos numa ótica geral. Os criminosos digitais brasileiros agem em campos diversos, como roubo de identidade, fraudes de cartão de crédito, violação de propriedade intelectual e protestos políticos.

De acordo com levantamento realizado pela jornalista Fernanda K. Ângelo (2002), cópias de *software*, dados protegidos por direitos autorais e pirataria, bem como o vandalismo *on-line*, são alguns dos métodos ilícitos cada vez mais adotados por *hackers* brasileiros.

Tem-se, destarte, que a proliferação de ferramentas gratuitas para ataques, as poucas leis para a prevenção dos crimes digitais e o crescente índice de grupos organizados para explorar oportunidades para o *cybercrime* são as principais causas apontadas pelo estudo para o aumento dessas ações na internet (ÂNGELO, 2002).

Ademais, a evolução da internet e o aumento desenfreado da informatização fazem com que os crimes praticados pela internet, também denominados "crimes virtuais" sejam cada vez mais frequentes e difíceis de lidar no ordenamento jurídico brasileiro, dada a dificuldade de punir de forma eficaz os agentes devido, principalmente, à sensação de impunidade gerada.

Diante do exposto, o trabalho em questão ressalta a seguinte problemática: O que já foi legislado para combater os crimes virtuais vem resolvendo efetivamente os chamados "crimes cibernéticos" ou apenas pequena parte do *iceberg* que é a onda desses crimes?

A referida legislação, infelizmente, se mostra ineficiente e ineficaz para atender a demanda, cada dia maior dos delitos dessa natureza, mesmo diante das mudanças significativas ocorridas no direito brasileiro, com o intuito de sanar a dificuldade em identificar a autoria dos delitos praticados na internet.

Importante salientar que o enfoque principal do presente trabalho, intitulado de "Crimes Cibernéticos", consiste na análise das previsões penais – normativas expressas na Lei nº 12.737/2012, os quais passarão a ser estudadas, minuciosamente, a seguir, enfatizando-se os seus principais elementos constitutivos, bem como o posicionamento dos Tribunais Superiores pátrios acerca da mencionada temática.

A escolha deste tema se deu em razão da necessidade de debaterem-se os "Crimes Cibernéticos", sobretudo em razão da grande proporção de que a chamada "era informática" tomou no atual cenário social. Ademais, a presente temática visou analisar a Lei nº 12.737/2012, conhecida como Lei "Carolina Dickmann", importante instrumento de coerção aos crimes praticados no ambiente virtual.

2 A INTERNET COMO FERRAMENTA DE COMUNICAÇÃO INTERPESSOAL

A nova ferramenta de comunicação interpessoal alavancou formas instantâneas de relacionamentos, facilitando assim, a vida em sociedade, a qual está em constantes transformações. A cada geração, mudam-se os modos de convívio, sendo o sistema informatizado considerado a "vanguarda da globalização".

2.1 DO CONCEITO DE INTERNET

A interligação de pessoas por meio da rede de computadores proporciona o acesso as mais variadas informações, que, na visão de Joshua Eddings (1994 apud DULLIUS, 2012, [n.p.]):

> É uma sociedade cooperativa que forma uma comunidade virtual, estendendo-se de um extremo a outro do globo. Como tal, a internet é um portal para o espaço cibernético, que abrange um universo virtual de ideias e informações em que nós entramos sempre que lemos um livro ou usarmos um computador, por exemplo.

A internet é um método de comunicação em nível global, proporcionando elos entre os computadores conectados à rede, os quais são protocolos de conexão, também conhecidos como TCP/IP, que em inglês significam *Transmission Control Protocol/Internet Protocol.* Tais protocolos foram desenvolvidos pelo *Advanced Research Project Agency* (ARPA), e estipulam regras a serem seguidas pelos computadores que se comunicam entre si ou com computadores de outra rede (WIKI, 2014).

Assim, como em uma sociedade organizada, em que as pessoas físicas e/ou jurídicas possuem cadastros com finalidade de controle por meio de um número, CPF's e CNPJ's respectivamente, que os identificam e diferenciam uns dos outros de uma forma registrada e disciplinada, também ocorre na rede mundial de computadores, em que cada computador possui seu próprio registro, conhecido como endereço IP. Tal endereço torna possível que todas as ações desenvolvidas por dada máquina sejam registradas e monitoradas.

Popularmente conhecida como *web*, trata-se de um mecanismo que possibilita "manejar" as informações na internet. "[...] É um sistema de documentos dispostos na Internet que permitem o acesso às informações apresentadas no formato de hipertexto. Para ter acesso a tais informações pode-se usar um programa de computador chamado navegador" (MARTINS, 2008). Outrossim, verifica-se, na atualidade, o crescimento em grande escala deste tipo de mecanismo, proporcionando, assim, interligações anteriormente inatingíveis a níveis global.

2.2 ORIGEM HISTÓRICA E DEFINIÇÕES DA REDE MUNDIAL DE COMPUTADORES

A rede mundial de computadores interligada de forma virtual, por meio da internet, pessoas em volta do planeta, sendo considerada a "mãe" de todas as conexões, que se originou de um projeto militar norte americano. Vejamos:

> O governo norte-americano queria desenvolver um sistema para que seus computadores militares pudessem trocar informações entre si, de uma base militar para a outra e que mesmo em caso de ataque nuclear os dados fossem preservados. Seria uma tecnologia de resistência. Foi assim que surgiu então a ARPANET, o antecessor da internet, um projeto iniciado pelo Departamento de Defesa dos Estados Unidos que realizou então a interconexão de computadores, através de um sistema conhecido como comutação de pacotes, que é um esquema de transmissão de dados em rede de computadores no qual as informações são divididas em pequenos "pacotes", que por sua vez contém trecho de dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original. (SILVA; MONTEIRO, 2009, [n.p.]).

Com o passar do tempo, várias pequenas redes começaram a utilizar a tecnologia desenvolvida pela ARPANET. "O estabelecimento do Protocolo de Comunicação (The Internet Protocol-IP) foi o que possibilitou a existência da internet e permitiu que qualquer quantidade de computadores fosse interligada em rede" (GOUVEIA, 1997).

A internet é um marco na divisão da história da humanidade, principalmente, pela quantidade de benefícios que proporciona, mas também, por estar se tornando um instrumento de crime, tem causado ao homem muitas preocupações. O cyber espaço infelizmente tem como realidade a disseminação das ações criminosas contribuindo tanto para a geração de novos delitos quanto para a execução de crimes já conhecidos.

2.3 ASPECTOS POSITIVOS DA INTERNET

A internet mudou a comunicação em todo o mundo e está cada vez mais presente em nossa rotina, influenciando em nossa vida nos mais variados aspectos: político, econômico, lazer, investigação, comércio e serviços on-line, educação, enfim, nas mais diversas áreas de nossa sociedade.

No que tange à busca de informações, a internet é a preferida entre os usuários. Dentro dela está a World Wide Web (WWW) que, baseando-se em arquivos de hipertexto em uma linguagem chamada HTML e por meio do uso de um protocolo específico (HTTP) onde é possível o compartilhamento de informações, disponibilizando-as à busca por parte dos interessados.

No entendimento de José Manuel Moran (2003 apud DILLIUS,2012, [n.p.]):

> Uma das características mais interessantes da Internet é a possibilidade de descobrir lugares inesperados, de encontrar materiais valiosos, endereços curiosos, programas úteis, pessoas divertidas, informações relevantes. São tantas as conexões possíveis, que a viagem vale por si mesma. Viajar na rede precisa de intuição acurada, de estarmos atentos para fazer tentativas no escuro, para acertar e errar. A pesquisa nos leva a garimpar joias entre um monte de banalidades, a descobrir pedras preciosas escondidas no meio de inúmeros sites publicitários.

Conforme Valzacchi (2003, p. 129-177), a utilização da internet em aulas pode chegar a ser proveitoso, para ele:

> Aprender a aprender e a desenvolver a criatividade são habilidades críticas na sociedade onde o conhecimento se renova com velocidades inesperadas. Através de diálogos entre os pares, entre alunos e professores ou em comunidades de aprendizes.

Na educação, é possível acessar informações em qualquer lugar do mundo, ou seja, podemos pesquisar informações em bibliotecas, universidades, livrarias, doutrinadores, entre outros.

2.4 CRIMINALIDADE NA REDE

Proporcionalmente aos benefícios que surgiram com a internet vieram, também, condutas ilícitas praticadas por agentes especializados nesse campo. Tais comportamentos são conhecidos de diversas formas, tais como crimes virtuais, crimes

cibernéticos, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, crimes de internet, fraude informática, crimes transnacionais, entre outras.

Nesse âmbito, temos a figura do criminoso informático, que possui inteligência, conhecimento de sistemas de informações e usos de meios informatizados com o fim de atingir bens jurídicos alheios, fazendo-se valer de um novo universo de possibilidades de atuação criminosa.

O Direito Penal encontra muitas dificuldades de adaptação dentro deste contexto. Senão, vejamos:

> O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é justamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, desenvolvida por agentes que se aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores. (PINHEIRO, 2009 apud DULLIUS, 2012, [n.p.]).

O ciberespaço é um lugar imaginário, que só temos acesso pelo computador, mesmo assim precisa estar ligado à realidade pelo uso que temos feito dele nos dias atuais, transformando-o em um espaço intermediário entre o mundo imaginário e o mundo real. Nas lições de Cecílio da Fonseca Vieira Ramalho Terceiro (2009 apud DULLIUS, 2012, [n.p.]):

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido a ausência de seus autores e seus asseclas.

O que se percebe é que o crime virtual é qualquer conduta antijurídica e culpável, realizada a partir de um computador conectado à internet. Segundo Augusto Eduardo de Souza Rossini (2004 apud DULLIUS, 2012, [n.p.]):

> O conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Para o autor supramencionado, "delito informático" é gênero, do qual "delito telemático" é espécie, dada a peculiaridade de ocorrer no e a partir do interrelacionamento entre os computadores em rede telemática usados na prática delitiva (ROSSINI, 2004 apud DULLIUS, 2012).

Ainda, a respeito do tema assevera Rossini (2004 apud DULLIUS, 2012) a denominação "delitos informáticos" abarca crimes e contravenções penais, alcançando não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos. Isto também ocorre nas situações em que o computador seria uma mera ferramenta, sem a imprescindível "conexão" à internet. Percebe-se, portanto, pelo explanado que a criminalidade na rede de informática com o passar do tempo vem tendo outro dimensionamento perante a revolução social, causando entraves inatingíveis pelo regramento até então em vigor, do que será pautado no capítulo seguinte.

3 CLASSIFICAÇÃO DOS CRIMES VIRTUAIS E SEUS SUJEITOS

Os Crimes virtuais podem ser classificados em próprios ou puros e, ainda, em impróprios ou impuros. Senão, vejamos:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. (FERREIRA apud CARNEIRO, 2012, [n.p.]).

Didaticamente falando, a classificação mais adequada a atual realidade é a que os crimes podem ser próprios ou impróprios.

3.1 CRIMES VIRTUAIS PRÓPRIOS

Os crimes virtuais próprios são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime.

Nessa categoria de crimes está, não só a invasão de dados não autorizados, mas toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos.

Para alguns doutrinadores, como Marco Túlio Viana, crimes virtuais próprios "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)" (VIANA, 2003 apud CARNEIRO, 2012).

Corroborando com esse conceito, valiosas são as lições de Damásio Evangelista de Jesus (apud CARNEIRO, 2012, [n.p.]):

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

3.2 CRIMES VIRTUAIS IMPRÓPRIOS

Os crimes virtuais denominados impróprios são aqueles realizados com a utilização do computador, ou seja, por meio da máquina que é utilizada como instrumento para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado, crimes, portanto que já tipificados que são realizados agora com a utilização do computador e da rede, utilizando o sistema de informática seus componentes como mais um meio para realização do crime, e se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado como no caso de crimes como: pedofilia.

Do mesmo modo afirma o jurista Damásio E. de Jesus (2012 apud CARNEIRO, 2012, [n.p.]). *In verbis*:

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Essas classificações são eficazes didaticamente para se entender e classificar alguns crimes, mas por conta da rapidez na evolução e dinâmica da rede de computadores e internet fica quase impossível acompanhar e afirmar categoricamente que não há modalidades que não estejam elencadas nas classificações adotadas.

3.3 SUJEITO ATIVO

A imputação objetiva ao autor do crime e sua comprovação é extremamente difícil frente à ausência física do sujeito ativo. Ocorre que, frente à importância da

identificação do autor do crime e a dificuldade desta identificação, surgiu a necessidade de se traçar um perfil denominando grupos que praticam determinados crimes virtuais, dentre essas denominações temos a figura do *hacker*.

O significado literal da palavra *hacker*, segundo tradução do dicionário Michaelis (2009), quer dizer, "pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados". Ou seja, tecnicamente pessoas com conhecimentos ímpares sobre informática e sistemas que se utilizam de seus conhecimentos não necessariamente para práticas ilícitas, a partir do momento que se vislumbra que *hackers* são pessoas com grande conhecimento, é possível haver conhecimento técnico de forma positiva e negativa.

Com isso entende-se que *hacker* é apenas o gênero, e as espécies de *hackers* podem variar de acordo com as práticas, uma das espécies são os *crackers*; essa palavra foi criada no ano de 1985, por *hackers* que não concordavam com a utilização do termo *hacker* pela imprensa para definir técnicos ou usuários de computadores que incorressem em ações ilegais ou que causassem transtornos para outras pessoas.

Os *hackers* e os *crackers* geralmente são muito parecidos em relação ao vasto conhecimento aprofundado em informática, sendo que a principal distinção é a finalidade que suas práticas resultam, posto que os *hackers* realizam atividades positivas, não criminosas, enquanto a motivação dos *crackers* é criminosa em sua essência, agindo, normalmente e premeditadamente, com objetivo criminoso de obter vantagens ilícitas.

Dentre essas espécies temos ainda os chamados *lamers*, titulados de *wannabes* ou *script-kid*, são *hackers* que atuam em pequenos feitos, limitando seus conhecimentos e não representam tanto perigo sendo classificados como leigos frente às grandes posições de hackers, ainda nas espécies temos os *phreakers* que comentem crimes específicos voltados para a área de telecomunicações e os defacers que registram suas marcas ao invadirem páginas na internet e desfigurá-las.

Frente à classificação desses perfis de criminosos temos uma ideia de quem eles são, o que querem de uma forma genérica e como agem, mas a pergunta é como identificá-los antes mesmo deles cometerem condutas ilícitas que os identifiquem, já que quando falamos em sujeito ativo sabemos que realmente os dados obtidos para identificação do sujeito é o endereço da máquina que envia as informações, ou seja, o IP, seu login e senha, portando com a possibilidade de camuflagem dos dados e a utilização de dados inverídicos dificilmente há uma rápida identificação do sujeito ativo na prática.

3.4 SUJEITO PASSIVO

Quando falamos de um crime específico, logo sabemos quem é o sujeito ativo e passivo da conduta quem realizou e em quem recaiu a ação ou omissão. Contudo, no caso dos crimes virtuais, de forma generalizada, a única afirmação cabível é que será sempre uma pessoa física ou jurídica ou uma entidade titular seja pública ou privada titular do bem jurídico tutelado, sempre haverá o sujeito passivo, ou seja, alguém que está sendo lesado enfim o que sofre a ação.

Portanto, o sujeito passivo da infração penal pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica, haja vista poder, por exemplo, ter seus bens desviados, seu patrimônio deteriorado ou mesmo ter informações violadas. Ambas são capazes de determinar a ação do agente criminoso.

Ocorre que, atualmente muitos dos crimes praticados ainda não são divulgados, seja por conta da não disseminação dessas informações ou pela falta de denúncias, como, por exemplo: grandes empresas evitam a divulgação sobre possíveis ataques virtuais ou mesmo invasões para não demonstrarem fragilidade quanto à segurança, e quanto às pessoas físicas vemos que por falta da devida punibilidade aos infratores e a falta de mecanismos de denúncia, apesar de já existirem, as vítimas acabam não denunciando o que facilita a propagação desses crimes.

4 CLASSIFICAÇÃO DOUTRINÁRIA DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos são classificados pela doutrina brasileira dominante como delito de natureza formal, posto que se consumam no momento da prática da conduta delitiva, independente da ocorrência do resultado naturalístico.

Ademais, e com muita propriedade acerca desse tema, o jurista Vicente de Paula Rodrigues Maggio (2013, [n.p.]) assim classificou os crimes cibernéticos. In verbis:

> Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), *plurissubsistente* (costuma se realizar por meio de vários atos), *comissivo* (decorre de uma atividade positiva do agente: "invadir", "instalar") e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de *forma vinculada* (somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de *forma livre* (pode ser cometido por qualquer meio de execução), conforme o caso, *formal* (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer), *instantâneo* (a consumação não se

> prolonga no tempo), *monossubjetivo* (pode ser praticado por um único agente), *simples* (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima).

5 CONTEÚDO DA LEI E CONDUTAS PUNÍVEIS

A Lei nº 12.737/2012 – Lei dos Crimes Cibernéticos, ou, também conhecida como, a Lei "Caroline Dickmann", trouxe importantes alterações ao Decreto-Lei 2.848/40 – Código Penal brasileiro, ao passo que realizou a formalização e a tipificação de condutas delituosas no âmbito informático, constituindo os chamados "crimes cibernéticos".

Importante se faz tecer algumas considerações acerca da suso mencionada Lei no tocante aos seus respectivos artigos.

A tipificação dos crimes informáticos está prevista no primeiro artigo do referido diploma legal, mas, valendo-se da hermenêutica jurídica, onde se lê "crimes informáticos", devem ser interpretados como "crimes cibernéticos".

Já o seu segundo artigo, por sua vez, realizou alterações na seção IV do Código Penal brasileiro, que trata dos crimes contra a inviolabilidade dos segredos, posto que se acrescentou ao compêndio penal os artigos 154-A e 154-B.

Destaque-se que ambos os artigos de Lei buscam proteger de quaisquer violações os dispositivos informáticos, senão vejamos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2ºAumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3ºSe da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a

> conduta não constitui crime mais grave.
> § 4ºNa hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5ºAumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

O *caput* do dispositivo acima transcrito (art. 154-A do CP) pode ser considerado o maior avanço proporcionado por essa norma. Isso porque, seu objetivo principal é realizar o combate às principais práticas danosas, conhecidas por trazerem transtornos para quem se utiliza ou necessita dessas tecnologias.

De mais a mais, os novos artigos inseridos no Código Penal brasileiro pela Lei 12.737/2012 buscam combater a invasão de dispositivos informáticos alheios, conectados ou não à rede de computador. Importante salientar que se entende por dispositivos informáticos: computador de mesa, *notebook, laptop, ultrabook, tablete, ipad, smartphone* etc.

O tipo penal indica, ainda, a necessidade de o dispositivo informático possuir algum mecanismo de segurança, sob pena de ser considerado desprotegido penalmente (NUCCI, 2013, p. 742).

Assim, tem-se, então, que para cometer a conduta tipificada no referido artigo o sujeito ativo deverá invadir, ou seja, violar/transgredir o dispositivo alheio, sem precisar necessariamente estar conectado com a rede de computadores, e com a finalidade de obter, adulterar ou destruir dados ou informações.

Outrossim, na previsão trazida pelo § 1º, o qual elenca como condutas do tipo normativo produzir, oferecer, distribuir, vender ou difundir, constituem práticas que dependem das condutas típicas previstas no *caput* do artigo 154-A, isto é, para cometer a conduta tipificada neste parágrafo, o sujeito deverá reunir os elementos objetivos e subjetivos do tipo.

De mais a mais, os parágrafos 2º ao 5º do referido artigo, preveem formas qualificadas pelo resultado, as quais, em síntese, serão assim configuradas se a invasão tiver como resultado a obtenção de conteúdo de comunicações eletrônicas privadas,

segredos comerciais ou industriais ou sigilosos ou controle remoto não autorizado do dispositivo invadido, sendo que, nestas hipóteses, a pena será de reclusão de seis meses a dois anos, e multa. Contudo, caso haja a divulgação, comercialização ou transmissão a terceiros dos dados obtidos mediante as referidas condutas delitivas, a pena será aumentada de um a dois terços.

Nesse mesmo sentido, aumenta-se de um terço ou até a metade se o crime cometido for praticado contra o Presidente da Republica, governadores e prefeito, Presidente do STF, o da Câmara dos Deputados e Senador, o da Assembleia Legislativa, o presidente da Câmara Legislativa do Distrito Federal e Municipal e contra pessoas que possuam "cargos máximos" da administração pública direta e indireta, seja qual for à esfera.

Vale ressaltar, ainda, que os crimes contra inviolabilidade dos segredos possuem previsão constitucional, advindo da proteção da intimidade e da vida privada da pessoa (BRASIL, 1988, art. 5º, inciso X).

Não podemos esquecer-nos, também, do art.154 B do CP, sendo este acrescentado, como já vimos anteriormente, mediante a redação do segundo artigo da referida lei.

Destaque-se que este artigo traz a identificação da natureza da ação penal, dispondo, como regra geral aplicável aos crimes cibernéticos, a ação penal pública condicionada à representação, ou seja, aquela em que a vitima deverá autorizar expressamente a autoridade policial para realizar as investigações e o membro do Parquet a iniciar a persecução penal.

Entrementes, a ação penal será pública incondicionada, ou seja, não terá necessidade de representação da vitima, quanto à conduta for praticada em desfavor da administração pública direta ou indireta em qualquer esfera da União.

Algumas considerações acerca do terceiro artigo da mencionada lei, o qual alterou a redação do art. 266 do CP, incluindo à figura do tipo normativo o serviço informático, telemático ou de informação de utilidade pública, prevendo, ainda, que a interrupção ou perturbação das novas formas de comunicação é crime (OLIVEIRA, 2013).

O legislador pátrio pensou bem no momento dessa atualização, uma fez que se fazia necessária devido às novas transformações da "era cibernética".

Os elementos objetivos do tipo são: interromper, perturbar, impedir ou dificultar, isto é, o sujeito deverá impossibilitar a execução, atrapalhar ou romper o serviço, não havendo, inclusive, elementos subjetivos de tipo específico.

No tocante às formas qualificadas pelo resultado, assim considerado quando o crime for praticado em época de calamidade pública, a pena a ser aplicada será em dobro.

Já ao artigo 298 do CP foi acrescentado o parágrafo único, o qual realizou a equiparação entre o cartão de crédito e de débito com documentos particulares (COSTA, 2012).

O quarto artigo da Lei "Carolina Dickman", por fim, traz disposições acerca da vacatio legis, estipulando que a norma entraria em vigor em 120 (cento e vinte) dias após a sua publicação oficial.

6 AÇÃO PENAL E A APURAÇÃO DOS DELITOS INFORMÁTICOS

"Crime" consiste na conduta que lesa os direitos individuais e sociais do indivíduo e da sociedade, respectivamente. Sendo assim, importante salientar as lições do ilustre doutrinador Noberto Avena (2014, p. 224):

> A sua prática gera ao Estado o poder-dever de punir. Como esta punição não pode ser arbitrária nem ocorrer à revelia das garantias individuais do indivíduo são necessárias a existência de uma fase prévia de apuração, assegurando-se ao possível responsável o direito de defesa, o contraditório e a produção de provas.

No tocante aos Crimes Cibernéticos, assim dispõe a Lei nº 12.737/2012, em seu artigo 154-A. *Ipsis litteris:*

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Ocorre que as disposições impostas pela citada lei referiram-se, também, ao tipo de ação penal cabível quando da prática de delitos de natureza cibernética, os quais foram elencados no artigo 154-A, acima transcrito. Essa é a inteligência do artigo 154-B da Lei 12.737/2012. In verbis:

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido

> contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Necessário explanar que o artigo 154-B estabelece que as práticas criminosas previstas no dispositivo 154-A (crimes cibernéticos) só se procederão por intermédio de representação do ofendido. Nestes casos, a ação penal será pública, condicionada à representação da vítima, observando-se para tanto a legitimidade e o prazo decadencial. Contudo, ressalvaram-se, ainda, às hipóteses em que os crimes ocorrem contra a administração pública direta ou indireta da União, Estados, Municípios e Distrito Federal, ou, ainda, contra empresas concessionárias de serviços públicos, posto que a ação penal será de natureza pública incondicionada.

Assim sendo, o artigo 154–B se presta a situar qual tipo de ação penal que deve ser movida para que a vítima tenha a devida tutela jurisdicional e, consequentemente, ocorra a sanção do sujeito ativo do crime.

7 CONCLUSÃO

Com a evolução da internet e, consequentemente, diante das transformações de paradigmas sociais, em conjunto com o aumento desenfreado da informatização, a celeuma envolvendo incidentes cibernéticos é matéria que nunca perde sua importância, de modo que se tornou necessária a elaboração de uma lei que dispunha acerca da tipificação criminal de delitos informáticos.

Assim, diante desse contexto, surgiu a Lei nº 12.737/12, a qual fora devidamente analisada neste trabalho acadêmico, que traz em seu bojo a tipificação do crime denominado "Invasão de dispositivo informático".

Diversas questões relacionadas à aludida Lei, que acabou sendo "apelidada" com o nome da atriz Carolina Dieckmann, foram abordadas com o objetivo de esclarecer as principais dúvidas porventura existentes a respeito do tema em epigrafe.

Ademais, fazendo-se um retrospecto de forma sucinta, é possível verificar características dos crimes cibernéticos que são indispensáveis para o bom entendimento do tema. Dessa forma, sabe-se que o primeiro passo do presente estudo consistiu em tecer breves comentários acerca da história/evolução do assunto em comento.

Vários aspectos relacionados à internet foram expostos de forma clara e objetiva, entre eles a origem histórica, definições da rede mundial de computadores, aspectos da internet e criminalidade na rede. Foi explicado, também, a classificação dos crimes virtuais e seus sujeitos, quais sejam, os crimes virtuais próprios e impróprios, sujeito ativo e passivo.

No que tange à ação penal prevista no artigo 154-B, que trata do impulso inicial acusatório a ser realizado quando da prática de um dos tipos penais, nos caso, dos crimes do caput do artigo 154-A, a ação penal será pública condicionada à representação da vítima. Dito de outro modo, levando em conta a natureza do ilícito praticado e o interesse geral da sociedade, o legislador outorgou para a vítima o oferecimento da condição de procedibilidade, observando-se a legitimidade e o decurso do prazo decadencial.

Todavia, a ação penal se converterá em pública incondicionada quando a infração penal for praticada contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (art. 154-B da Lei nº 12.737/12).

De todo o amealhado, resta concluir que, proporcionalmente aos benefícios que surgiram com a internet vieram, também, condutas ilícitas praticadas por agentes especializados neste campo.

Assim, a entrada em vigor da contemporânea Lei nº 12.737/12, representou significativa mudança no nosso ordenamento jurídico, haja vista tratar de crimes cada vez mais constantes na hodierna sociedade, tipificando condutas que não eram previstas, de forma específica, como infrações penais.

Ressalte-se que, apesar da legislação aludida objetivar suprir lacunas no Direito brasileiro, ainda, permanecem lapsos no ordenamento vigente a serem preenchidos, haja vista que o texto da Lei em comento permite várias interpretações, além disso, as reduzidas penas aumentam as chances do Estado perder o direito/dever de punir mediante a ocorrência da prescrição.

Importante frisar que, diante do contexto atual que apresenta crescente índice de crimes virtuais, bem como as falhas ainda existentes na legislação, faz-se essencial a educação/conscientização das pessoas em respeitar a intimidade/privacidade alheia, objetivando, assim, evitar a ocorrência/vitimização de delitos informáticos.

REFERÊNCIAS

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF, 3 out 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 21 nov. 2014.

BRASIL. **Constituição da república federativa do Brasil de 1988**. Brasília: Palácio do Planalto. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 21 nov. 2014.

BRITO, Auriney. **Análise da Lei 12.737/12 – "Lei Carolina Dieckmann"**. Disponível em: <http://politicacidadaniaedignidade.blogspot.com.br/2013/04/analise-da-lei-1273712-lei-carolina.html>. Acesso em: 21 nov. 2014.

CAPEZ, Fernando. **Curso de direito penal. Vol. 2, dos crimes contra a pessoa a dos crimes contra o respeito aos mortos (arts. 121 a122)**. 12.ed. São Paulo: Saraiva, 2012.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, Rio Grande, XV, n.99, abr. 2012. Disponível em:<http://www.ambitojuridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17>. Acesso em: 22 nov. 2014.

CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2.ed. Rio de Janeiro: Lumen Juris, 2003.

CAVALCANTE, Márcio André Lopes. **Comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático**. Disponível em: <http://marciocavalcante2.jusbrasil.com.br/artigos/121942716/comentarios-a-lei-12737-2012-que-tipifica-a-invasao-de-dispositivo-informatico>. Acesso em: 20 nov. 2014.

COSTA, Sandro. **O cibercrime e as leis 12.735/2012 E 12.737/2012**. Disponível em: <http://www.infonet.com.br/sandrocosta/ler.asp?id=137447>. Acesso em: 22 nov. 2014.

DULLIUS, Aladio Anastácio. **Dos crimes praticados em ambientes virtuais**. 2012. Disponível em: <http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html>. Acesso em: 22 nov. 2014.

FERNANDA K. ANGELO. Brasil lidera ranking mundial de hackers e crimes virtuais. **Folha Online.** Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml>. Acesso em: 20 nov. 2014.

FRANCESCO, Wagner. **O que você precisa saber sobre a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann"**. Disponível em: <http://wagnerfrancesco.jusbrasil.com.br/artigos/152372896/o-que-voce-precisa-saber-sobre-a-lei-12737-2012-conhecida-como-lei-carolinadieckmann?utm_campaign=news letterdaily_20141120_336&utm_medium=email&utm_source=newsletter>. Acesso em: 21 nov. 2014.

GOUVEIA, Sandra Medeiros Proença. **O direito na era digital: Crimes praticados por meio da informática**. Rio de Janeiro: Mauad, 1997. Disponível em: <http://books.google.com.br/books?id=3vzmW3DtAuQC&pg=PA43&lpg=PA43&dq=o+legislador+come%C3%A7ou+a+se+preocupar+com+o+mau+uso+dos+recursos+da+inform%C3%A1tica&source=bl&ots=TDsESpVdyx&sig=H-FP7BDOai9J5BzdZjtElpc0SU8&hl=pt-BR#v=onepage&q=o%20legislador%20come %C3%A7ou%20a%20se%20

preocupar%20com%20o%20mau%20uso%20dos%20recursos%20da%20inform%C3%A1tica&f=false>. Acesso em: 22 nov. 2014.

MAGGIO, Vicente de Paula Rodrigues. **Novo crime**: invasão de dispositivo informático - CP, Art. 154-A. Disponível em: <http://vicentemaggio.jusbrasil.com.br/ artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a>. Acesso em: 22 nov. 2014.

MARTINS. Elaine. **O que é wold wide web?** 2008. Disponível em: <http://www.tecmundo.com.br/web/759-o-que-e-world-wide-web-.htm>. Acesso em: 22 nov. 2014.

MIRANDA, Marcelo Baeta Neves. **Abordagem dinâmica aos crimes via internet**. Disponível em: <http://www.charlieoscartango.com.br/cot-diversos-artigobaeta.html>. Acesso em: 22 nov. 2014.

MONTEIRO, J; SILVA. D. **História da Internet**. 2009. Disponível em: <http://pt.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 22 nov. 2014.

NUCCI, Guilherme de Souza. **Manual de direito penal.** 9.ed. São Paulo: Revista dos Tribunais, 2013.

OLIVEIRA JÚNIOR, Eudes Quitino de. **A nova Lei Carolina Dieckmann**. Disponível em: <http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>. Acesso em: 21 nov. 2014.

OLIVEIRA, Natacha Alves de. **Crimes praticados pelo sistema de informática:** visão prospectiva e sistemática à luz da jurisprudência pátria. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=13587>. Acesso em: 21 nov. 2014.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002.

SENADO FEDERAL. **Lei nº 12.737/2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 nov. 2014.

SCHMIDT, Guilherme. Crimes cibernéticos. **Jusbrasil**, 2014. Disponível em: < http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 20 nov.2014.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

VALZACCHI, Jorge R. **Internet y educacion**: aprendiendo y ensensando em los espacios virtuales. 2.ed. Versão Digital, 2003. Disponível em: <http://www.educoas.org/portal/bdigital/es/indice_valzacchi.aspx>. Acesso em: 22 nov. 2014.

VIEIRA, Alexandre Pires; ALVES, José Cláudio Rodrigues. **O direito à privacidade frente aos avanços tecnológicos na sociedade da informação**. Disponível em: <http://jus.com.br/artigos/27972/o-direito-a-privacidade-frente-aos-avancos-tecnologicos-na-sociedade-da-informacao/2#ixzz3K70lVeRz>. Acesso em: 20 nov. 2014.

Data do recebimento: 2 de Janeiro de 2015
Data da avaliação: 2 de Janeiro de 2015
Data de aceite: 12 de Janeiro de 2015

1 Acadêmica do Curso de Direito da Universidade Tiradentes – UNIT. Campus de Estância.
E-mail: jessicalmeida@hotmail.com.br
2 Acadêmica do Curso de Direito da Universidade Tiradentes – UNIT. Campus de Estância.
E-mail: allana-barbosa@hotmail.com
3 Acadêmico do Curso de Direito da Universidade Tiradentes – UNIT. Campus de Estância.
E-mail: gilmarcarmo@yahoo.com.br
4 Acadêmico do Curso de Direito da Universidade Tiradentes – UNIT. Campus de Estância. E-mail: ken_ss@hotmail.com
5 Acadêmica do Curso de Direito da Universidade Tiradentes – UNIT. Campus de Estância.
E-mail: luana.munique@hotmail.com
6 Acadêmica do Curso de Direito da Universidade Tiradentes – UNIT. Campus de Estância.
E-mail: robertarayanne_se@hotmail.com